STATUS OF CLAIMS

Claims 1 - 28 are pending.

Claims 1 – 28 stand rejected.

REMARKS

Information Disclosure Statement

An information disclosure statement is being submitted herewith for the Examiner's consideration.

35 U.S.C. 103(a) Rejections

Claims 1 – 28 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro (United States Patent No. 6,009,176) in view of Bjerrum (United States Patent No. RE.36,310). Applicant respectfully requests reconsideration and removal of these rejections for at least the following reasons.

35 U.S.C. §103(a) sets forth in part:

> [a] patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

To establish a prima facie case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art. *See, MPEP 2143.03; see also, In re. Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).* Further, there

must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings. *See, M.P.E.P. 706.02(j).* Further yet, the teaching or suggestion to make the claimed combination must be found in the prior art, and not based on the applicant's own disclosure. *In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).* Applicant respectfully submits a proper motivation for combining the references as argues is lacking for at least the following reasons.

Claim 1 recites, in part,

> [a] method for securely exchanging information items used to generate encryption keys among at least two parties using a public/private encryption key system over a communications network ... comprising the steps of: ... determining a next encryption key.

Gennaro is directed to authenticating digital streams. *See, e.g., Abstract, lines 1 – 3.* To authenticate a digital stream, Gennaro proposes computing and verifying a single digital signature on a portion of the stream. *See, Abstract, lines 3 – 5.* However, as the present Office action admits, Gennaro fails to teach, or even suggest for that matter, "determining a next encryption key", as is recited by Claim 1.[1]

In an attempt to remedy this admitted shortcoming of Gennaro, the present Office action relies upon the teachings of Bjerrum. However, Applicant respectfully

---

[1] Applicant notes the present Office action admits "Gennaro does not teach expressly determining a next encryption key from said next private key and said received information item, wherein said next encryption key is retained among said retained encryption keys." 09/09/2004 Office action, par. 6.

submits Bjerrum fails to remedy the deficiency of Gennaro for at least the following reasons.

Bjerrum is directed to a method of transferring data between computer systems using electronic cards. *See, Abstract.* Bjerrum expressly teaches,

> [t]he object of the present invention is to provide a method of the type defined above, according to which method it is possible to establish immediately a secure data or document transfer between two computer systems without having to exchange encryption/decryption keys between the computer systems, reveal details concerning security levels, etc., and according to which method it is ensured that the desired data or document transfer actually takes place, as it is ensured that it will not be possible for either of the parties or for a third party to interfere with the data or document transfer. *Col. 2, lines 5 – 14 (emphasis added).*

As this passage demonstrates, Bjerrum thus teaches the skilled artisan both the undesirability of, and a secure data transfer method that avoids, exchanging encryption/decryption keys between computer systems. Thus, Bjerrum teaches away from the use of exchanged security information. Accordingly, Applicant submits a proper motivation for combining the teachings of Gennaro and Bjerrum to reach the claimed invention is lacking.

That is, the Bjerrum reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention – i.e., its express teaching not to use exchanged security information. *See, W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984). As illustrated above, Bjerrum actually teaches away from the claimed invention – as Claim 1 expressly recites transmitting the next information

item over the communications network and determining the next encryption key from the received information item (in addition to the next private key). The determination of the next encryption key of Claim 1 uses a received information item while Bjerrum contradictorily teaches the undesirability of a method that exchanges keys or reveals data. As it is improper to combine references where the references teach away from their combination, Applicant submits it is improper to combine the Gennaro and Bjerrum references in an attempt to reach the claimed invention. *See, e.g., In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983)

Accordingly, Applicant respectfully requests reconsideration and removal of the rejection of Claim 1 for at least the reasons set forth above, namely, that a proper motivation for combining the references to meet the claimed invention is lacking. Applicant also respectfully requests reconsideration and removal of the rejections of Claims 2 – 10 as well, at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 1.

With regard to Claim 11, it analogously recites, in part, a processor operative to determine at least one next encryption key. Accordingly, Applicant respectfully requests reconsideration and removal of the rejection of Claim 11 for at least the foregoing reasons. Applicant also respectfully requests reconsideration and removal of the rejections of Claims 12 – 19 as well, at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 11.

With regard to Claim 20, it analogously recites, in part, "an encryption key generator to determine a next encryption key." Accordingly, Applicant respectfully requests reconsideration and removal of the rejection of Claim 20 for at least the

foregoing reasons. Applicant also respectfully requests reconsideration and removal of the rejections of Claims 21 – 28 as well, at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 20.

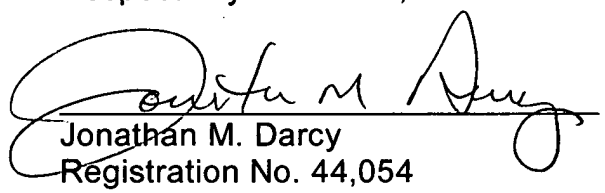
CONCLUSION

Wherefore, Applicant believes he has addressed all outstanding grounds raised in the outstanding Office action, and respectfully submits the present case is in condition for allowance, early notification of which is earnestly solicited.

Should there be any questions or outstanding matters, the Examiner is cordially invited and requested to contact Applicant's undersigned attorney at his number listed below.

Respectfully submitted,

Dated: December 9, 2004



Jonathan M. Darcy
Registration No. 44,054

Plevy, Howard & Darcy, P.C.
PO Box 226
Fort Washington, PA 19034
Tel: (215) 542-5824
Fax: (215) 542-5825